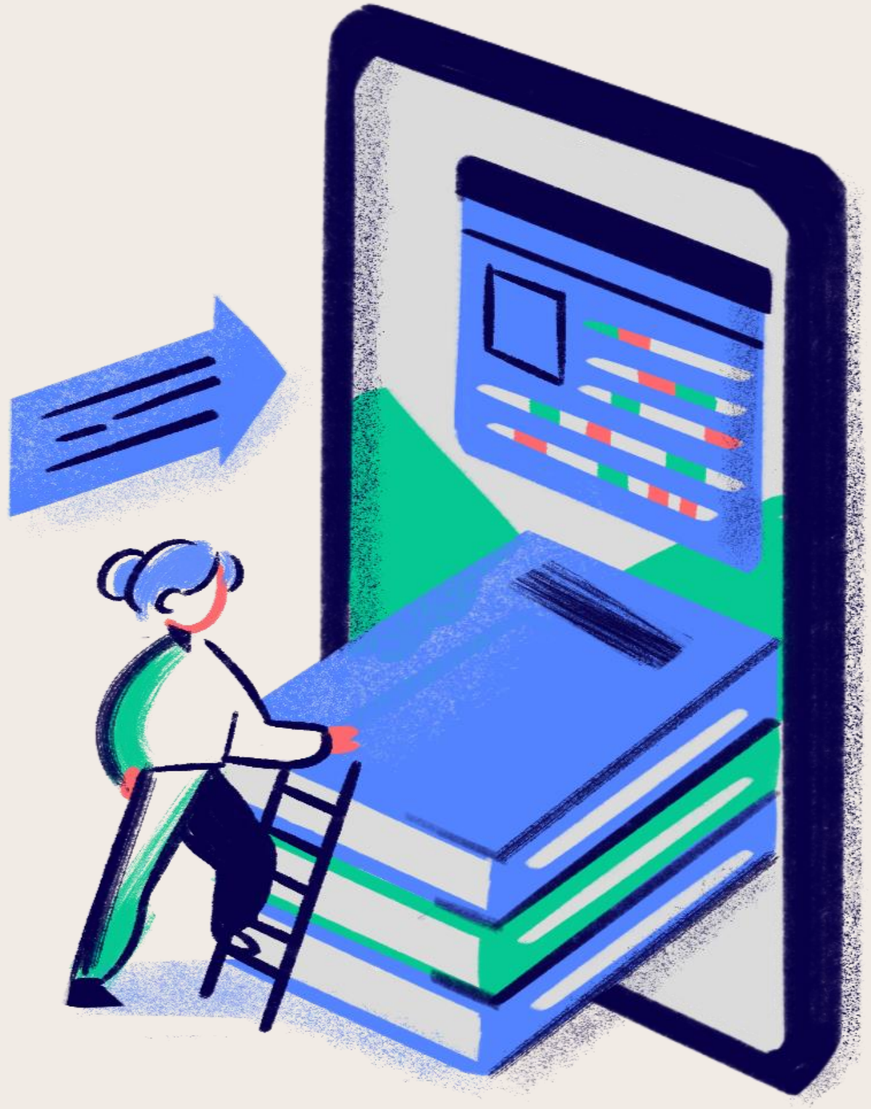
AI安全與隱私保護指南

課堂簡報



你知道什麼是生成式AI嗎？
(Generative AI)

想像一個神奇的廚師

給食材 → 做出料理

給指令 → 產生內容

為什麼他們那麼厲害？

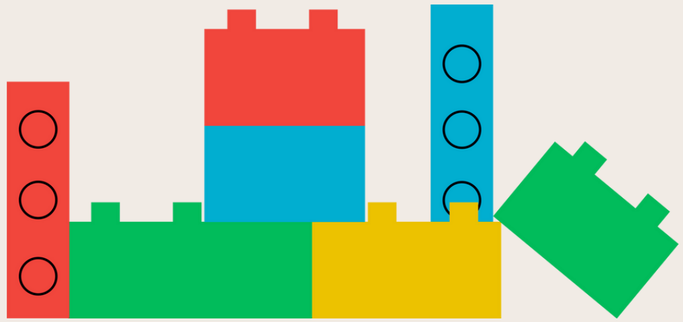
學過很多食譜

學過很多資料

生成式AI怎麼運作？

像是在玩樂高積木

第一步：學習（收集積木）



AI學習了很多資料
就像收集了很多不同的樂高積木

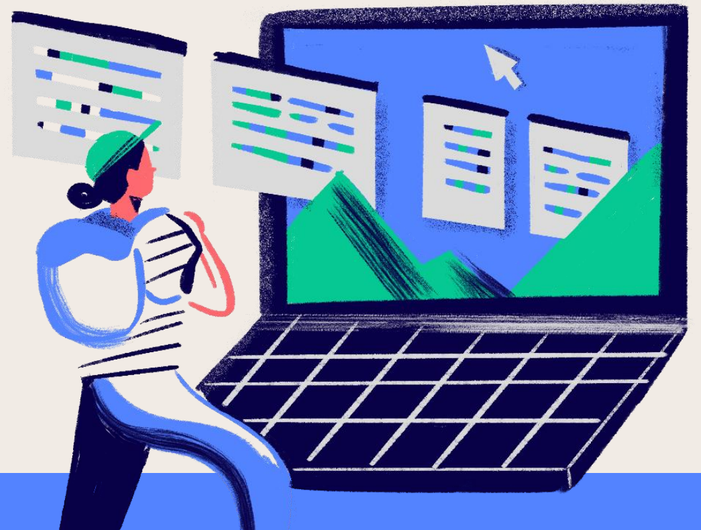
第二步：組合（拼積木）

AI把學到的東西重新組合
就像用積木拼出新的作品

第三步：創造（完成作品）

AI產生新的內容
就像用積木拼出前所未有的模型

生成式AI能做什麼事？



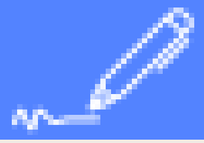
例如，生成式AI能做到

文字創作

回答問題

分析摘要

寫作文、腳本



圖像創作

畫風景

畫卡通

設計海報

影音創作

創作歌曲、編曲

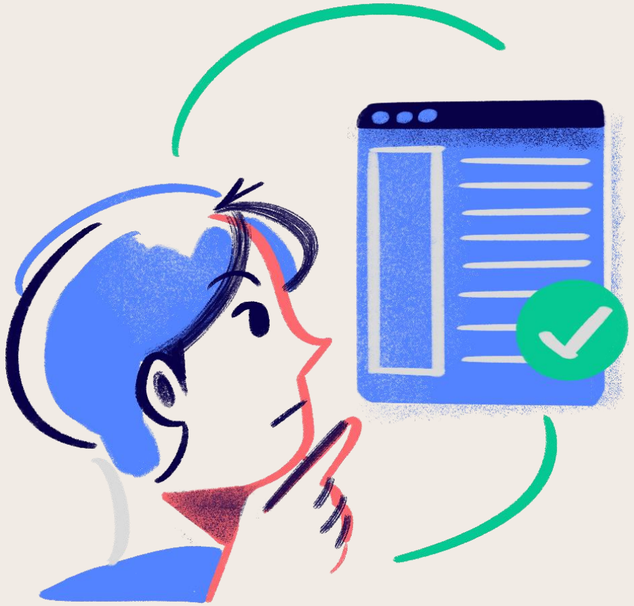
創作影像

程式創作

寫程式

發布網頁

不只這些.....



AI這麼強，
我們所有事都可以拜託它
？

以下哪一位同學使用AI是「不安全」的？

小美

目的：
寫一篇「我最喜歡的季節」作文

先在筆記本列出自己的想法：
喜歡春天
理由：天氣舒適、可以野餐
最愛看櫻花

詢問AI：
「我想寫一篇關於春天的作文，
可以請你幫我看看以下大綱合適嗎？
- 第一段：描寫春天的天氣
- 第二段：說明為什麼喜歡春天
- 第三段：分享賞花的經驗」

小明

目的：
想找人聊天、交朋友

先取得媽媽同意，可以和AI聊天

詢問AI：
「你好，我叫王小明，
住在台北市中山區xx路，
今年11歲，就讀xx國小五年三班，
我的電話是09xx-xxx-xxx，
星座：牡羊座 血型：O型
可以當我的朋友嗎？」

小華

目的：
製作「節能減碳」海報

先做資料研究：
- 查看課本內容
- 閱讀相關新聞

詢問AI：
「我正在製作節能減碳的海報，
想問問看一張好的科學海報應該包含哪些元素？
有什麼適合小學生的圖表建議嗎？」

小明這樣做，哪裡有問題？

小明

目的：
想找人聊天、交朋友

先取得媽媽同意，可以和AI聊天

詢問AI：
「你好，我叫王小明，
住在台北市中山區xx路，
今年11歲，就讀xx國小五年三班，
我的電話是09xx-xxx-xxx，
星座：牡羊座 血型：O型
可以當我的朋友嗎？」

- ✕ 提供真實姓名
- ✕ 透露完整住址
- ✕ 分享電話號碼
- ✕ 洩露就讀學校
- ✕ 過度信任AI

再考考你，那小花這樣做呢？

小花　喜歡攝影和繪畫，最近發現AI可以改變照片風格

目的：

想要做出特別的畢業照

第一步：上傳照片

小花上傳了：

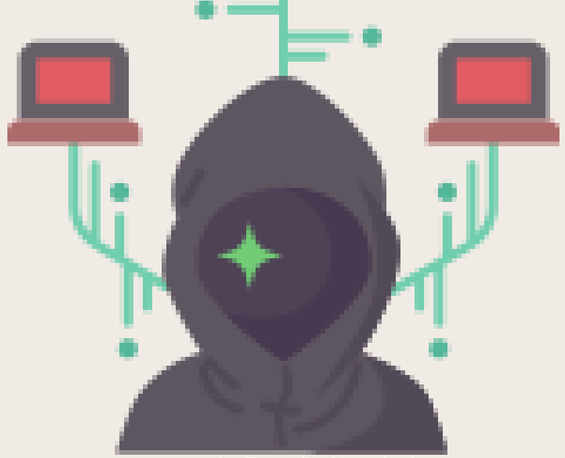
- 自己的證件照
- 學校生活照
- 全家福照片
- 同學合照

第二步：向AI輸入

「請幫我把這些照片：

1. 變成動漫風格
2. 改成超級英雄造型
3. 製作成各種表情貼圖
4. 放到不同的背景中」

小花危險行為分析



主要風險

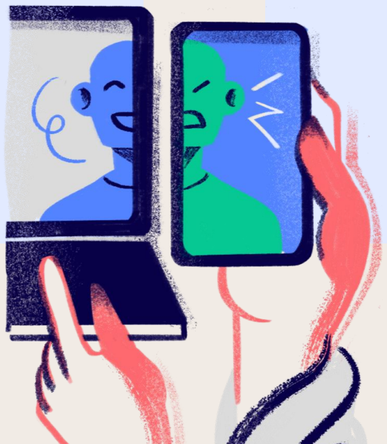
- 個人肖像外流
- 照片可能被儲存
- 可能被用於其他用途
- 難以追蹤照片去向

他人隱私侵犯

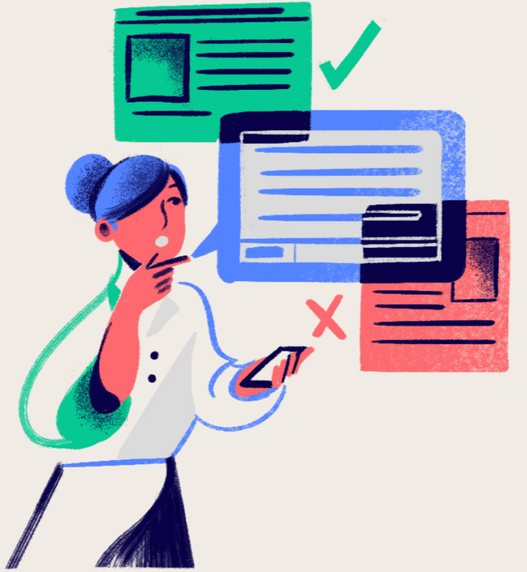
- 未經同意使用同學照片
- 全家福包含家人肖像
- 違反他人肖像權

可能的後果

- 上傳就無法完全刪除
- 照片可能被濫用
- 可能被AI學習和記錄
- 產生不當改圖
- 造成同學困擾
- 引起家人擔心



使用AI 的基本原則



01. 保持透明

- 要知道我們在用什麼 AI 工具
- 了解這些工具怎麼運作
- 清楚知道誰在管理我們的資料

02. 資料最小化

- 想像 AI 工具像是陌生人
- 不要告訴它太多個人資訊
- 只提供必要的資料

03. 明智選擇

- AI 很有幫助，但不是萬能的
- 要獨立思考，不要完全依賴 AI
- 對 AI 的回答保持懷疑態度

保護自己的方法

個人資料保護，不要告訴 AI：

- 真實姓名
- 家庭住址
- 就讀學校、學號
- 生日
- 電話號碼

安全使用小技巧

- 使用好的密碼
- 定期更換密碼
- 不要在不同網站用同一個密碼
- 使用前先看清楚 AI 工具要求什麼權限

保護個人肖像的原則

- 視同個人資料保護
- 不上傳真實照片
- 不隨意分享生成圖片
- 尊重他人肖像權
- 有疑慮先詢問師長

安全使用小技巧

- 使用文字描述
- 避免提供具體特徵
- 下指令時，文字敘述保持適當模糊
- 注意AI軟體使用條款

負責任地使用 AI

要做的事

- 用 AI 幫助思考
- 驗證 AI 的答案
- 保持自己的想法
- 遵守班級和學校規定

不要做的事

- 用 AI 寫作業
- 抄襲 AI 的答案
- 用 AI 製造假訊息
- 騙人或傷害他人

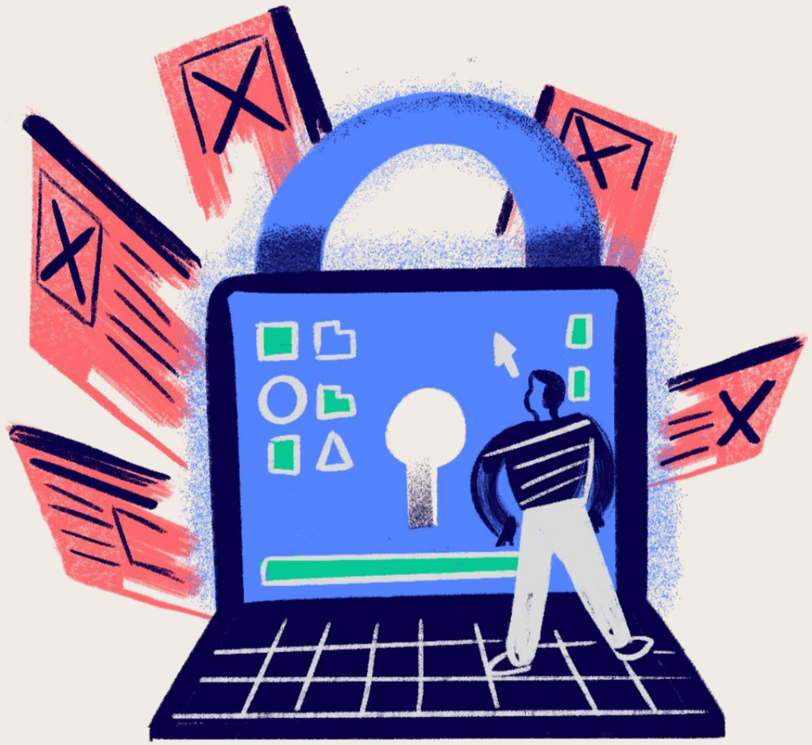
常見問題

AI 會記住我說的話嗎？

有些 AI 會記錄對話
有些會忘記對話
最好假設它會記住，所以要小心說話

AI 的答案可信嗎？

AI 有時候會說錯
要查證重要資訊
避免偏見與歧視的敘述
不要完全相信 AI 的答案



安全使用

AI是工具，不是玩具

安全第一，效率第二

有問題隨時詢問老師